



CVE-2018-14368

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-14368
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-19 02:29:00 UTC
Updated	2023-11-07 02:52:00 UTC
Description	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the Bazaar protocol dissector could go into an infinite loop. T

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference

[SECURITY] [DLA 1451-1] wireshark security update
Wireshark · wnpa-sec-2018-40 · Bazaar dissector infinite loop
code.wireshark Code Review - wireshark.git/commit
Wireshark Bugs in Multiple Dissectors Let Remote Users Cause the Application to Crash or Consume Excessive CPU Resources - SecurityTr
Wireshark Multiple Denial of Service Vulnerabilities
[security-announce] openSUSE-SU-2020:0362-1: moderate: Security update f
code.wireshark Code Review - wireshark.git/commit
14841 – Buildbot crash output: fuzz-2018-06-07-8554.pcap
CVE Program record

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296066](#) Oracle Solaris 11.4 Support Repository Update (SRU) 40.107.3 Missing (CPUOCT2021)

[377461](#) Alibaba Cloud Linux Security Update for wireshark (ALINUX2-SA-2020:0078)

[501310](#) Alpine Linux Security Update for wireshark

[670216](#) EulerOS Security Update for wireshark (EulerOS-SA-2021-1859)

[670911](#) EulerOS Security Update for wireshark (EulerOS-SA-2021-1859)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)